

AFFIDAVIT

1:22 MJ 4385

I, Shadron Starnes, Special Agent of the Federal Bureau of Investigation (FBI), hereinafter referred to as your Affiant, being duly sworn, state that:

1. Your Affiant is an investigative or law enforcement officer of the United States within the meaning of Section 2510 (7), of Title 18, United States Code, as a Special Agent of the FBI. As such, your Affiant is empowered to conduct investigations of, and to make arrests for, offenses enumerated in Title 18, United States Code, Section 2516.

2. Your Affiant has been a Special Agent with the Federal Bureau of Investigation (FBI) since September 2018. Affiant has been employed by the FBI since October of 2011. Prior to becoming a Special Agent with the FBI, Affiant was employed as an Investigative Specialist within the FBI, assigned to work counterintelligence, counterterrorism, and cyber-crime matters. Affiant attended the FBI Academy in Quantico, Virginia from September 2018 to February 2019 where Affiant received basic criminal and organized crime training as well as drug/narcotics training. In February 2019, Affiant was assigned to investigate organized crime matters in the Cleveland Division. Affiant has participated in investigations and prosecutions involving the following types of offenses: fraud; the distribution of illegal drugs; money laundering offenses; crimes of violence; firearms violations; international and domestic organized criminal activities; and cyber-crime activities.

3. As a result of your Affiant's personal participation in this investigation and reports made to your Affiant by other Special Agents of the FBI, USPIS, and other state and local law enforcement officers, witnesses and reliable confidential sources, your Affiant is familiar with the circumstances and offenses described in this Affidavit.

4. This affidavit is offered in support of a criminal complaint against DAVID JAMES SMITH for the offenses detailed below. The information in this Affidavit is based on

Affiant's personal knowledge, information provided by other law enforcement officers and individuals, and the reports and memoranda of other law enforcement officers. The information in this affidavit is provided for the limited purpose of establishing probable cause related to the commission of a federal offense. The information is not a complete statement of all the facts relating to this case.

DEFINITIONS OF TECHNICAL TERMS USED IN THIS AFFIDAVIT

5. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."

6. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks). Examples of computer hardware include, but are not limited to, central processing units, laptop, desktop, notebook or tablet computers, computer servers, peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media, related communications devices such as modems, routers and switches, and electronic/digital

security devices, wireless communication devices such as mobile or cellular telephones and telephone paging devices, personal data assistants (“PDAs”), smart phones, iPods/iPads, Blackberries, digital cameras, digital gaming devices, global positioning satellite devices (GPS), and portable media players.

7. “Computer software,” as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

8. “Computer passwords, pass-phrases and data security devices,” as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password or pass-phrase (a string of alpha-numeric characters) usually operates as a sort of digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

9. “Hyperlink” refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

10. “Attachment” refers to a data file (examples include Microsoft Word, PDF, or picture file) that, when included with an email, transfers the file directly to the recipient(s) of the email.

11. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

12. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone-based dial-up, broadband based access via digital subscriber line (“DSL”) or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a username or screen name, an “e-mail address,” an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an ISP over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

13. “Internet Protocol address” or “IP address” refers to a unique number used by a computer to access the Internet. IP addresses can be “dynamic,” meaning that the Internet Service Provider (“ISP”) assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

14. “Internet Protocol address” or “IP address” is a unique numeric address used to identify computers on the Internet. The standard format for IP addressing consists of four numbers between 0 and 255 separated by dots, e.g., 149.101.10.40. Every computer connected to the Internet (or group of computers using the same account to access the Internet) must be assigned an IP address so that Internet traffic, sent from and directed to that computer, is directed properly from its source to its destination. Internet Service Providers (ISPs) assign IP addresses to their customers’ computers.

15. “TOR” or “TOR Network”, also known as the “Onion Router”, is a network of computers designed to facilitate anonymity. Tor was originally designed, implemented, and deployed as a project of the U.S. Naval Research Laboratory for the primary purpose of protecting government communications. It is now available to the public at large. Information documenting what Tor is and how it works is provided on the publicly accessible Tor website at www.torproject.org. In order to access the Tor network, a user must install Tor software either by downloading an add-on to the user’s web browser or by downloading the free “Tor browser bundle” available at www.torproject.org. The Tor software protects users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address which could otherwise be used to identify a user. It prevents someone attempting to monitor an Internet connection from learning what sites a user visits, prevents the sites the user visits from learning the user’s physical location, and it lets the user access sites which could otherwise be blocked. Because of the way Tor routes communications through other computers, traditional IP identification techniques are not viable. When a user on the Tor network accesses a website, for example, the IP address of a Tor “exit node,” rather than the user’s actual IP address, shows up

in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP back through that Tor exit node IP. In that way, using the Tor network operates similarly to a proxy server – that is, a computer through which communications are routed to obscure a user's true location.

16. End-to-end encryption is a system of communication where only the communicating users can read the messages. Generally speaking, it prevents third parties – including through telecom providers, Internet providers, and even the provider of the communication service – from being able to access the cryptographic keys needed to decrypt the conversation. The systems are designed to defeat any attempts at surveillance or tampering because only the parties privy to the communication can decipher the data being communicated or stored. Companies that use end-to-end encryption are generally unable to hand over texts of their customers' messages to the authorities.

BACKGROUND CONCERNING DARK NET AND CRYPTOCURRENCY INVESTIGATIONS

17. The "clear" or "surface" web is part of the internet accessible to anyone with a standard browser and that standard web search engines can index. The deep web is the part of the internet whose contents are not indexed by standard web search engines. The dark net is a part of the deep web that not only cannot be discovered through a traditional search engine, but also has been intentionally hidden and is inaccessible through standard browsers and methods.

18. Dark net marketplaces operate on the dark net. These sites are generally only accessible through the input of specific addresses in a TOR browser. The dark net marketplaces function primarily as black markets, selling or brokering transactions involving drugs, cyber-arms, weapons, counterfeit currency, stolen credit card details, forged documents, unlicensed

pharmaceuticals, steroids, and other illicit goods as well as the occasional sale of legal products. Dark net vendors (also known as distributors) operate on these dark net markets as sellers of these goods. They provide detailed information about their wares on these sites, including listings of their drugs for sale, contact information (such as TOR-based email or encrypted messaging applications), and the prices and quantities of drugs for sale. Items purchased through dark net vendors are generally paid for in cryptocurrency such as Bitcoin. Cryptocurrency or virtual currency permits the anonymous exchange of unlimited amounts of digital currency to anyone in the world without the use of traditional banks or banking systems. Customers purchase these goods using a computer or smartphone.

19. Your Affiant is aware that some dark net marketplace vendors conduct the entirety of their transactions on the dark web marketplace. Other vendors use the sites as an advertising base and messaging system and conduct their financial business in peer-to-peer¹ transactions in order to avoid using third party escrow systems that they believe could be subject to law enforcement seizures as well as thefts, hacks, and scams.

20. Bitcoin (BTC)² is a type of virtual currency, circulated over the internet. Bitcoin are not issued by any government, bank, or company, but rather are controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin is just one of many varieties of virtual currency. Other currency includes Bitcoin Cash (“BCH”), Litecoins (“LTC”), Ethereum (“ETH” or “ether”), and Ripple (XRP). For ease of reference, the analysis below

¹ A “peer-to-peer” transaction is a direct transaction between two individuals without a third party intermediary.

² Since Bitcoin is both a currency and a protocol, capitalization differs. Accepted practice is to use “Bitcoin” (singular with an uppercase letter B) to label the protocol, software, and community, and “bitcoin” (with a lowercase letter b) to label units of the currency. That practice is adopted here.

relating to Bitcoin generally applies to other types of cryptocurrencies (often collectively referred to as “Altcoins”).

21. Bitcoin are sent to and received from BTC “addresses.” A Bitcoin address is somewhat analogous to a bank account number and is represented as a case-sensitive string of letters and numbers. Each Bitcoin address is controlled through the use of a unique corresponding private key. This key is the equivalent of a password, or PIN, and is necessary to access the Bitcoin address. Only the holder of an address’ private key can authorize any transfers of bitcoin from that address to other Bitcoin addresses. Users can operate multiple BTC addresses at any given time and may use a unique Bitcoin address for each and every transaction.

22. To acquire bitcoin, a typical user purchases them from a virtual³ currency exchange. A virtual currency exchange is a business that allows customers to trade virtual currencies for other forms of value, such as conventional fiat money (*e.g.*, U.S. dollars, Russian rubles, euros). Exchanges can be brick-and-mortar businesses (exchanging traditional payment methods and virtual currencies) or online businesses (exchanging electronically transferred money and virtual currencies). Virtual currency exchanges doing business in the United States are regulated under the Bank Secrecy Act and must collect identifying information about their customers and verify their clients’ identities.

23. To transfer bitcoin to another Bitcoin address, the sender transmits a transaction announcement, which is electronically signed with the sender’s private key, across the peer-to-peer BTC network. To complete a transaction, a sender needs only the Bitcoin address of the receiving party and the sender’s own private key. This information on its own rarely reflect any

³ Bitcoins can accurately be referred to as a virtual, digital, and/or cryptographic currency.

identifying information about either sender or recipient. As a result, little-to-no personally identifiable information about the sender or recipient is transmitted in a Bitcoin transaction itself. Once the sender's transaction announcement is verified by the network, the transaction is added to the blockchain, a decentralized public ledger that records every Bitcoin transaction. The blockchain logs every Bitcoin address that has ever received bitcoin and maintains records of every transaction for each Bitcoin address.

24. While a Bitcoin address owner's identity is generally anonymous within the blockchain (unless the owner opts to make information about the owner's Bitcoin address publicly available), investigators can use the blockchain to identify the owner of a particular Bitcoin address. Because the blockchain serves as a searchable public ledger of every Bitcoin transaction, investigators can sometimes trace transactions to third party companies that collect identifying information about their customers and are responsive to legal process.

25. In addition to Bitcoin and other cryptocurrencies, there are also tokens. Like Bitcoin and Altcoins, tokens use blockchain technology. Tokens are digital assets that are powered through smart contracts. While tokens theoretically can be used to represent any assets that are fungible and tradeable, they are often used as a commodity similar in some ways to stocks or options. In these scenarios, tokens are created and distributed through an Initial Coin Offering (ICO). Through an ICO, a venture offers a stock of specialized crypto tokens for sale with the promise that those tokens will operate as the medium of exchange when accessing services on a digital platform developed by the venture. The sale of tokens provides capital to fund the initial development of the digital platform, although no commitment is made as to the price of future services (in tokens or otherwise). In this sense, tokens are a fungible and

potentially highly volatile unit of value that can be easy to obtain. Your affiant is aware that dark net distributors are increasingly using tokens as a means of laundering their illicit gains.

26. Your affiant is aware that individuals conducting business in this manner must use a computer or other electronic device, such as a smartphone, tablet, or computer to conduct transactions involving cryptocurrencies or tokens. Users of cryptocurrencies or tokens must establish electronic wallets to receive and send the bitcoin during these transactions. These wallets are electronic in nature and may be stored on mobile devices (phones or tablets), external or removable media, or computers. They may also be stored on third party wallet providers (such as Armory). Individuals often associate email accounts with these wallet providers and store information relating to that wallet on their email account. Your affiant is also aware that individuals conducting business by bitcoin can back-up wallets to paper printouts that would contain information to restore the wallet in an electronic form (cold storage). Passwords for access to electronic wallets are typically complex and are often written down or saved in an accessible manner on paper or on some electronic device. They are also often stored on email accounts, cloud or shared drives stored online (such as Google Drive), and other online storage mediums.

27. Your affiant is aware that dark net marketplace accounts like those on the Dream Market have affiliated cryptocurrencies (including, but not limited to, Bitcoin) associated with the account. These cryptocurrencies – which are wholly owned by the account owner(s) – are often held in escrow on servers affiliated with the marketplace.

FACTS AND CIRCUMSTANCES REGARDING PROBABLE CAUSE

28. Since September 2021, investigators from FBI and United States Postal Inspection Service have been investigating the darknet vendor Squiintzzz. As of October 28,

2021, Squiintzzz had approximately 253 transactions with a 91% positive feedback within the ToRReZ marketplace. Within the user profile in this marketplace, Squiintzzz advertised Jabber account squiintzzz@jabb3er.de for communications.

29. Law Enforcement identified an Instagram account using the username “squiintzzz” and the name David Smith Sr. (hereinafter SMITH). The profile was publicly viewable and contained multiple images of a white male. A public post from on or around May 4, 2020, contained the pictured below of the white male.



30. United States Postal Service's (USPS) databases identified an account registered under the username squintzzz1 to an Ashley Lopez (hereinafter Lopez) with email address squiintzzz@outlook.com, telephone number 215-398-2824, and address 405 E. High Street, Philadelphia, Pennsylvania. Additional analysis identified an account with username

squintzzz@icloud.com⁴ that was registered to Lopez with an email address of diiindiiin@icloud.com and address 436 N. 9th Street, Apt. 3, Philadelphia, Pennsylvania. An additional search of USPS databases resulted in the discovery of three other accounts believed to be linked to the above accounts. Each of the additional three accounts were also registered to Lopez, telephone number 215-398-2824, email address diiindiiin@icloud.com, and address 6030 Lindbergh Blvd., Philadelphia, Pennsylvania.

31. On January 3, 2022, investigators served legal process on Apple requesting records associated to accounts connected to email address diiindiiin@icloud.com, squiintzzz@icloud.com, and telephone number 215-398-2824.

32. Records provided by Apple on or about January 24, 2022, revealed an Apple account associated to email address diiindiiin@icloud.com and telephone number 215-398-2824 registered to SMITH, mail address 6030 Lindbergh Blvd Apt 2, Philadelphia, Pennsylvania which was created on June 30, 2021. This account was also associated to address 376 S Main St Apt 2, Phillipsburg, New Jersey within the records. Records also revealed an Apple account associated to email address squiintzzz@icloud.com registered to Squint Wagerzzz, mail address 405 E high Street, Philadelphia, Pennsylvania, and telephone number 215-397-0468 was created on January 25, 2021.

33. On March 25, 2022, an administrative subpoena was served on Kraken requesting records associated to SMITH, date of birth 05/14/1993, and various email addresses associated to SMITH.

⁴ Squintzzz@icloud.com was used as the username and not the email address for the account.

34. On or around April 13, 2022, Kraken⁵ provided subpoena returns associated with SMITH. A review of the results identified three accounts associated with SMITH. Account information is contained in the table below. For each account, SMITH's Pennsylvania identification card was provided along with a selfie of SMITH including the below image of SMITH holding his Pennsylvania identification card bearing number XXXXX176⁶.

User ID	Email Address	Account Name	Address
Squintzzz	wickedturbulence@gmail.com	David Smith	376 South Main Street, Apt 2, Phillipsburg, NJ
Squiintzzz	eaglesmith1066@gmail.com	David Smith	27 North Cameron Street, Harrisburg, PA
BeefHolyfield	squiintzzz@icloud.com	David Smith	376 S Main St, Apt 2, Phillipsburg, NJ



⁵ Kraken is a United States-based cryptocurrency exchange.

⁶ Areas of the identification card have been redacted to protect personal identifiable information.

35. A review of SMITH's criminal history shows prior convictions for terroristic threats, unlawful possession of a weapon, theft, possession/sale of hypodermic needle, use/possession with the intent to use drugs, and domestic violence charges since 2011. In Phillipsburg, New Jersey, in or around 2011, SMITH was arrested and subsequently sentenced to 60 months' confinement and 2 years of probation for terroristic threats and unlawful possession of a weapon. In or around 2016, SMITH was arrested in Pennsylvania and subsequently sentenced to three to six years' confinement for violation of parole retail theft and violation of parole simple assault. SMITH was released in 2019 under parole conditions. After violating his parole conditions, he was wanted for being a Pennsylvania parole absconder until being arrested in July 2022.

36. On or about December 9, 2021, an administrative subpoena was served on T-Mobile for subscriber information related to telephone number 215-398-2824. A review of the results, revealed that from April 19, 2021, to May 24, 2021, the telephone number was registered to Ashley Lopez, 12359 Lehigh Street, Easton, PA.

37. On or about December 9, 2021, and February 24, 2022, administrative subpoenas were served on AT&T for subscriber information and toll records related to telephone number 215-398-2824. A review of the results received on December 13, 2021, revealed that from May 24, 2021⁷, to October 25, 2021, the telephone number was registered to SMITH, 405 East High Street, Philadelphia, PA 19144.

38. In or around February 2022, Pennsylvania Department of Corrections Parole authorities provided Law Enforcement with records pertaining to SMITH. A review of the

⁷ The same day as the account for Ashley Lopez ended with T-Mobile.

records demonstrated that, in 2019, SMITH's mother, Hope Smith, was living at 376 S Main St., Phillipsburg, New Jersey.

39. On March 9, 2022, investigators received records pursuant to a federal court order served on Microsoft on January 4, 2022, for records associated to email account squiintzzz@outlook.com. The records revealed that email account squiintzzz@outlook.com was created on February 11, 2021, and registered to David Smith. Records also identified the following payment information for the account:

Payment Method	Name	Expiration Date	Billing Address
VISA x4700	hope smith	08/2024	376 S Main St Apt 2 Phillipsburg, nj 08865-3090
VISA x8405	David Smith	02/2025	376 S Main St Apt 2 Phillipsburg, nj 08865-3090
VISA x3109	Hope Smith	03/2025	376 S Main St Apt 2 Phillipsburg, nj 08865-3090
VISA x5892	David Smith	09/2025	6030 Lindbergh Blvd Philadelphia, PA 19142
MC x4188	David Smith	03/2026	376 S Main St Apt 2 Phillipsburg, nj 08865
MC x4182	David Smith	01/2026	376 S Main St Apt 2 Phillipsburg, nj 08865

40. In or around April 2022, Fulton Bank provided subpoena returns associated with SMITH. A review of the results identified a Platinum Money Market account and a Simply Checking account that were opened electronically on or around May 4, 2021, with the primary account holder as David Smith. The email account on file for SMITH was squiintzzz@outlook.com with an address of 405 E. High Street, Philadelphia, Pennsylvania. On or around May 6, 2021, a wire was transferred to SMITH's Fulton bank account for \$1,500. The wire originated from a Wells Fargo account associated with SMITH's mother and address 376

South Main Street, Apt 2, Phillipsburg, NJ⁸. Between on or around June 3, 2021, and August 9, 2021, twelve checks totaling around \$26,629 were made out to SMITH's mother from SMITH's checking account. All twelve checks were returned due to insufficient funds in SMITH's checking account.

41. In or around April 2022, Wells Fargo provided subpoena returns associated with SMITH. A review of the results identified a checking account and a Simply Checking account that were opened on or around June 9, 2020, for SMITH with a Pennsylvania driver's license XXXXX176. The address on file was 376 S Main Street, Apt 2, Phillipsburg, New Jersey.

42. On or around November 1, 2021, an undercover employee placed an order within the ToRReZ marketplace from vendor Squiintzzz for "2G of top notch ice" for approximately 0.0011474 BTC (\$70) to be shipped via USPS.

43. On or November 12, 2022, Law Enforcement received the above package which bore a label with a sender address of Jamie Jordan, 6011 Lindbergh Blvd, Philadelphia, PA. The package contained what appeared to be one mylar bag and a vacuum sealed bag in the mylar bag. The bag contained a white crystalline substance. On or around July 21, 2022, the Ohio Bureau of Criminal Investigation (BCI) laboratory provided a report confirming the parcel contained around 2.04 grams of Methamphetamine.

44. On or around November 26, 2021, an undercover employee placed an order within the ToRReZ marketplace from vendor Squiintzzz for "25 bags 'blue boys' stamped heroin" for approximately 0.00367195 BTC (\$200) to be shipped via USPS.

⁸ The same address was associated with SMITH's Kraken account.

45. On or around December 14, 2021, Law Enforcement received the above package which bore a label with a sender address of Joshua Whitley, 417 E High St, Philadelphia, PA. The package contained what appeared to be around 30 waxed paper enveloped stamped “no pain” and a black skull and bones containing white powder. On or around July 21, 2022, the Ohio BCI laboratory provided a report confirming the parcel contained 30 wax bindles of white powder. Testing of the powder from one bindle confirmed the bindle contained less than 0.1 gram of white powder that tested positive for para-fluorofentanyl⁹ and fentanyl.

46. On or around January 6, 2022, an undercover employee placed an order within the ToRReZ marketplace from vendor Squiintzzz for “20 bags of no pain stamped heroin xtremely potent” for approximately 0.004738 BTC (\$206) to be shipped via USPS.

47. On or around January 25, 2022, Law Enforcement received the above package which bore a label with a sender address of Jamie Jordan, 6011 Lindbergh Blvd, Philadelphia, PA. The package contained what appeared to be a mylar bag with a tied off Ziploc bag inside. The plastic bag contained a white powdery substance. On or around July 21, 2022, the Ohio BCI laboratory provided a report confirming the parcel contained around 6.55 grams of Cocaine HCL.

48. On or around January 31, 2022, an undercover employee placed an order within the Dark0de marketplace from vendor Squiintzzz for “10 bags of drive thru stamped china white pure!!! clone” for approximately 0.002946 BTC (\$113) to be shipped via United Parcel Services (UPS).

⁹ Parafluorofentanyl is an opioid analgesic analogue of fentanyl, sometimes referred to as ‘China-white’.

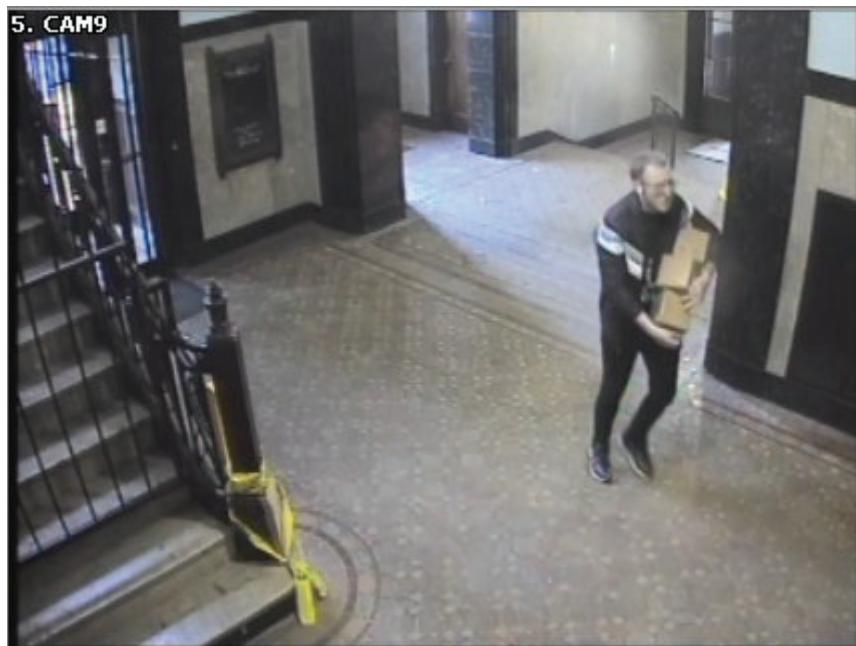
49. On or around February 7, 2022, Law Enforcement received the above package which bore a label with a sender address of Marcus Brown, 2 Kings Bridge Ct, Newark, Delaware, and tracking number ending 0442. The package contained what appeared to be one mylar bag which contained multiple small baggies. Inside each baggie was a waxed paper enveloped stamped “drive thru” containing white powder. On or around July 21, 2022, the Ohio BCI laboratory provided a report confirming the parcel contained 12 wax bindles of white powder. Testing of the powder from one bindle confirmed the bindle contained less than 0.1 gram of white powder that tested positive for fentanyl.

50. On or around April 7, 2022, UPS provided subpoena returns related to the above-mentioned package with tracking number ending 0442. A review of the results identified the package was shipped from Allentown, Pennsylvania. Additionally, the shipper profile within UPS for the package was created on or around February 2, 2022, with the name David Smith and address 31 S 9th St, Allentown, Pennsylvania.

51. On or around February 27, 2022, an undercover employee placed an order within the darknet marketplace Tor2Door from vendor Squiintzzz for “1g of Synthetic Heroin (dangerously potent)” for approximately 0.00597201 BTC (\$225) to be shipped via USPS.

52. On or around March 17, 2022, Law Enforcement received two USPS packages which bore the same labels. The labels contained a sender address of Jamie Jordan, 6011 Lindbergh Blvd, Philadelphia, Pennsylvania, and identical tracking numbers ending 1901. The packages were small brown boxes that each contained what appeared to be one mylar bag and a baggie of white powder in each mylar bag. On or around July 21, 2022, the Ohio BCI laboratory provided a report confirming the parcel contained around 2.07 grams total of fentanyl.

53. Law Enforcement was able to utilize the USPS tracking number ending 1901 to identify the packages were shipped from a Post Office in Allentown, Pennsylvania. Law Enforcement reviewed surveillance footage of the Post Office during the date and time the packages were shipped. Law Enforcement identified a white male that took three small brown boxes to the mail clerk to be shipped. The brown boxes appeared to be the same size and shape as the packages Law Enforcement received on March 17. Additionally, the white male appeared to be SMITH. A screenshot of the white male from the surveillance video is below.



54. On or around March 2, 2022, Pirate Ship provided subpoena returns related to known email addresses associated with SMITH including squintzzz@outlook.com. Pirate Ship allows users to purchase USPS and UPS postage through a variety of means including cryptocurrency. A review of the results identified Pirate Ship account 1769080 was created on or around August 21, 2021, and utilized squintzzz@outlook.com, phone number 484-861-8788, name Veronica Sanchez, and address 5000 S Broad St, Philadelphia, Pennsylvania. Account 1769080 had three different payment sources associated with the account including a prepaid

Visa card ending 2393 with the name David Smith on the card, a prepaid Visa card ending 9531 with the name Ashley Lopez on the card, and a Visa debit card ending 3908 with the name Hope Smith on the card. Pirate Ship account 1769080 created and shipped four different parcels on or around August 21 and 22, 2021, to addresses in Nevada, South Carolina, Texas, and Colorado.

55. Further review of the Pirate Ship returns identified account 1690972, which was created on or around July 12, 2021, and utilized email address diiindiiin@icloud.com, phone number 215-398-2824, name David Smith, and address 6030 Lindbergh Blvd Apt 2, Philadelphia, Pennsylvania. Account 1769080 had multiple payment sources associated with the account under the names SMITH, Lopez, and Lisa Burgos including prepaid Visa card ending 2393 with the name David Smith on the card which was also used by Pirate Ship account 1769080. Additional accounts were linked to accounts 1690972 and 1769080 as shown in the table below. Affiant knows that individuals involved in criminal activity frequently use multiple accounts to obfuscate law enforcement's ability to identify the individual and to track their activities.

Account	Email	Name	Address	Phone	Association
1769080	squiintzzz@outlook.com	Veronica Sanchez	5000 S Broad St, Philadelphia	484-861-8788	Same Payment as 1690972, 1743020, and 1783882
1690972	diiindiiin@icloud.com	David Smith	6030 Lindbergh Blvd Apt 2, Philadelphia	215-398-2824	Same Payment as 1769080, 1743020, 1831008, and 1783882
1743020	squiintzzz@icloud.com	Jessica Shmidt	312 E High St, Philadelphia	215-214-8587	Same Payment as 1690972, 1769080, and 1783882
1831008	squiintzzz@myself.com	Sammy Constantine	116 Locust Street, Philadelphia	267-777-0021	Same Payment as 1690972
1783882	squiintzzz@aol.com	Jessica Gonzalez	1521 E 7th St, Behlehem, PA	484-861-8788	Same Payment as 1690972,

				1769080, and 1743020
--	--	--	--	-------------------------

56. Pirate Ship Account 1690972 created around 188 labels to be shipped throughout the United States including the two packages Law Enforcement received in March 2022 with USPS tracking numbers ending 1901.

57. On or around March 23, 2022, an undercover employee placed an order within the darknet marketplace Tor2Door from vendor Squiintzzz for “3.5g of Synthetic Heroin (dangerously potent)” for approximately 0.0111355 BTC (\$475) to be shipped via USPS.

58. On or around March 28, 2022, an undercover employee sent a message to vendor Squiintzzz asking for the status of the order. On March 29, 2022, the undercover employee received a message from Squiintzzz indicating that it was delivered and provided the tracking number ending with: 7707. Additionally, Squiintzzz wrote “...we will be limited here while we are launching our new vendor onion site. Better prices and faster service. Store is live as of this morning.” Squiintzzz further provided the address ending o2kyd.onion.

59. On or around April 5, 2022, Law Enforcement received a package which bore tracking number ending 7707. The labels contained a sender address of Jamie Jordan, 6011 Lindbergh Blvd, Philadelphia, Pennsylvania. The package contained what appeared to be one mylar bag and a baggie of white powder in the mylar bag. On or around July 21, 2022, the Ohio BCI laboratory provided a report confirming the parcel contained around 3.41 grams of fentanyl.

60. Records obtained from United States Postal Inspection Services revealed that tracking number ending 7707 was being tracked from IP address 24.115.142.87 on the following dates and time:

03/25/2022	10:09:33 Central Time
03/26/2022	06:23:58 Central Time

61. On or around March 30, 2022, an administrative subpoena was served on PenTeleData for subscriber information related to the use of IP address 24.115.142.87 on the following dates:

03/25/2022 10:09:33 Central Time
03/26/2022 06:23:58 Central Time

A review of the results obtained on March 30, 2022, revealed the following account holder and address:

Account # 744481
David Smith
148 Arbor Way
Stroudsburg, PA 18360
610-773-5722
squintzzz@aol.com

62. On or around March 30, 2022, and April 5, 2022, an administrative subpoena was served on Verizon Wireless for subscriber information and toll records related to telephone number 610-773-5722. A review of the results revealed that since December 20, 2021, the phone number was registered to Ashley Lopez, 31 S. 9th St. Fl 2, Allentown, PA.

63. United States Postal Service's databases identified two accounts registered in or around May 2022 that utilized telephone number 610-773-5722. Both accounts were registered to SMITH, with email address comrade.aweigh_0x@icloud.com¹⁰ and address 148 Arbor Way, Stroudsburg, PA.

64. On or around March 31, 2022, investigators conducted surveillance at 148 Arbor Way and identified the following three vehicles in the premises:

¹⁰ Email address comrade.aweigh_0x@icloud.com was identified within records associated to email account diiindiiin@icloud.com. It appears that the "Hide My Email" function was used within the Apple iCloud account. According to the apple.com website "Hide My Email lets you create unique, random email addresses to use with apps, websites, and more so your personal email can stay private".

- a. Lincoln MKS bearing New Jersey license plate U52PKG – this vehicle was registered to Hope Smith
- b. BMW bearing New Jersey license plate S59PKG – this vehicle was registered to Hope Smith
- c. Nissan Murano bearing Pennsylvania license plate KXN3554 – this vehicle was registered to Alyza Rivera

65. On or around April 20, 2022, an undercover employee placed an order within the darknet marketplace Tor2Door from vendor Squiintzzz for “7g TOP NOTCH METH” for approximately 0.00400865 BTC (\$165) to be shipped via USPS.

66. On or around April 27, 2022, Law Enforcement received a package which bore tracking number ending 0645. The labels contained a sender address of Russel Smith, 317 S Main Street, Phillipsburg, NJ. The package contained what appeared to a sealed plastic bag containing a white crystalline substance within a mylar bag that was within another mylar bag. On or around August 30, 2022, the DEA North Central Laboratory provided a report confirming the parcel contained around 7.165 grams of methamphetamine hydrochloride

67. On or around May 4, 2022, PayPal provided subpoena returns associated to SMITH, Lopez, and known email addresses associated to them. A review of the returns identified account ending 4560 with the following identifiers: user name David Smith; email diiindiiin@icloud.com; phone number 610-773-5722; and addresses including 31 South 9th Street, Allentown, PA; 148 Arbor Way, Stroudsburg, PA; 19 Hilltop Dr, Wappingers falls, NY; and Apt 2 6030 Lindbergh Blvd, Philadelphia, PA. Multiple credit cards were linked to the PayPal account including a Master Card number ending 3906 from Coastal Community Bank with David Smith’s name on the card. Further review of the returns identified web and mobile

logins in April 2022 from IP Addresses including 104.28.55.178 on April 4, 2022, and 50.29.160.129 on April 7 and April 9, 2022 (as discussed below, these are associated with SMITH). Additionally, a review of transactions for the account identified around eight payments to Pirate Ship LLC between March 22 and 26, 2022.

68. On or around May 5, 2022, an undercover employee placed an order within the darknet marketplace Tor2Door from vendor Squiintzzz for “7g top notch meth” for approximately 0.00366016 BTC (\$135) to be shipped via USPS to an address in West Virginia.

69. On or around May 27, 2022, Law Enforcement in West Virginia¹¹ received a package which bore tracking number ending 0644. The labels contained a sender address of “James Todd, 19 hikltop dr., Wappingers Falls, NY 12590-3613”. The package contained what appeared to a sealed plastic bag containing a white crystalline substance within a mylar bag. The package contained approximately 8.8 grams of the white crystalline substance including the plastic bag. Law Enforcement field tested the substance with a TruNarc. The substance tested positive for Methamphetamine.

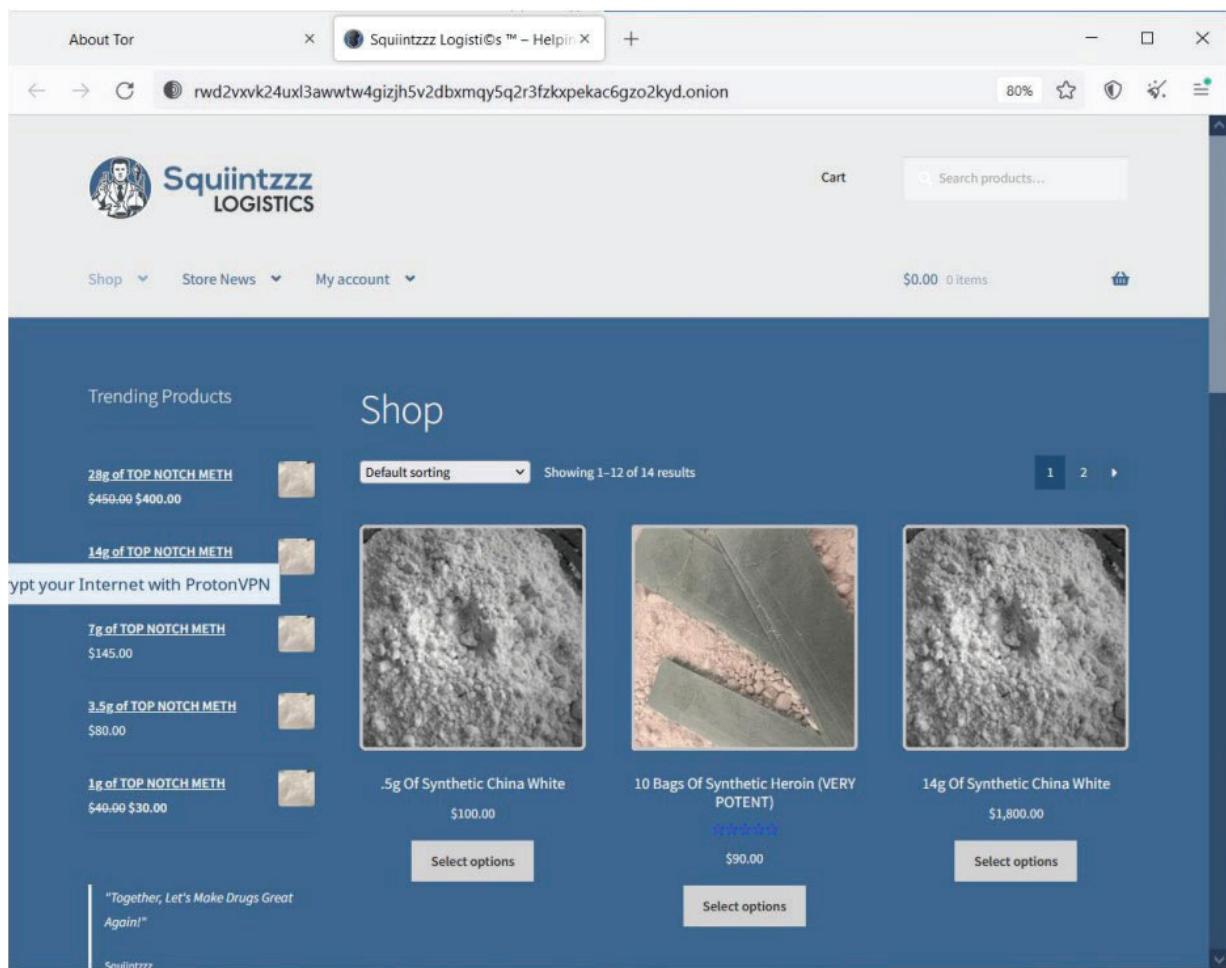
70. United States Postal Service’s databases revealed that tracking number ending 0644 was being tracked from IP address 24.115.143.47 on May 20, 2022, at 19:04:35 Central Time.

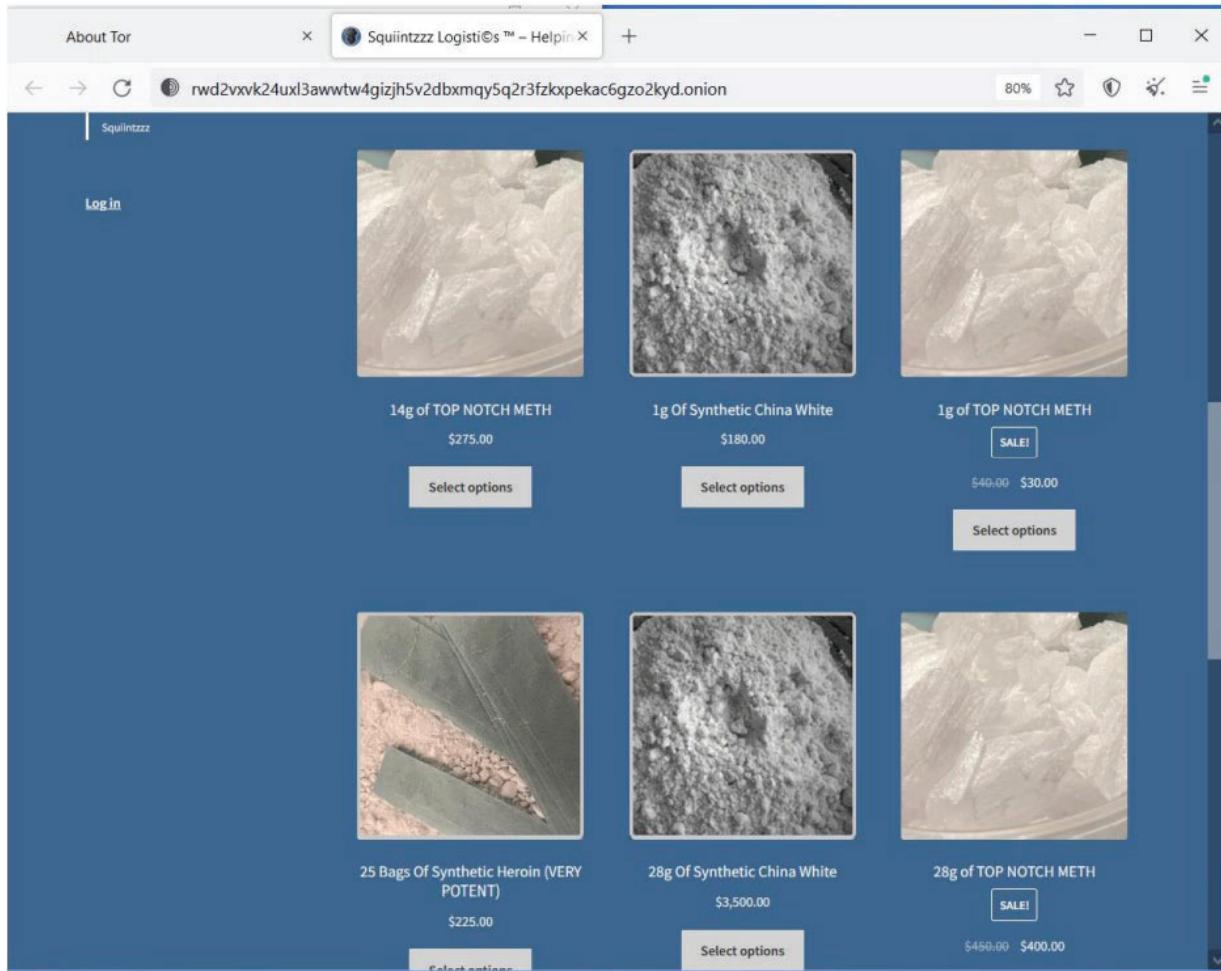
71. A review of updated subpoena returns from PenTeleData identified IP address 24.115.143.47 was utilized by Account # 744481¹² between May 17 and May 22, 2022.

¹¹ Every other package was shipped to and received in the Northern District of Ohio.

¹² Account # 744481 was still assigned to David Smith at 148 Arbor Way, Stroudsburg, PA.

72. On or around May 8, 2022, an undercover employee placed an order within the darknet shop Squiintzzz Logistics at address ending o2kyd.onion for “1g of Synthetic China White” for approximately 0.00526805 BTC (\$180) to be shipped via USPS. The BTC was sent to BTC address “...Ap4C1”. The product description stated “Disclaimer: This product contains fentanyl. The current ratio of our products is 90F/10H. We have the best 90/10 mix on the dark net,...” The URL for this shop was provided to undercover employee by the vendor Squiintzzz as a message within the Tor2Door marketplace. Screenshots of some of the products available on the site are below.





73. On or around May 16, 2022, Law Enforcement identified a publicly available Facebook profile for David Smith, Sr. The Facebook profile contained images of an individual that appeared to be SMITH including a photo of himself. On or around February 13, 2022, the profile posted that they started a new job as "Founder/Owner" of Squintzz Logistics.

74. On or around May 19, 2022, PenTeleData provided subpoena returns associated with account number 744481 which is associated with SMITH at Arbor Way. A review of the returns identified IP Address 104.28.55.178 was connected to account 744481 between March 17

and April 5, 2022 and IP Address 50.29.160.129 was connected to account 744481 between April 5 and April 12, 2022¹³.

75. On or around May 25, 2022, Zelle provided subpoena returns related to SMITH, LOPEZ and known email addresses associated with them. A review of the returns identified multiple profiles including the ones listed in the table below. From around March 6, 2022, to April 2, 2022, Zelle sender David Smith sent Grantland Aple around \$5,720. “Rent” was included in the memo line for multiple payments. On or around March 23, 2022, Grantland Aple sent SMITH two payments for \$2,000 with “Returning Over payment for rent” and “Return Rent over payment” in the memo line. Affiant believes SMITH was renting at Arbor Way from Grantland Aple.

RECIPIENT TOKEN	RECIPIENT FIRST NAME	RECIPIENT LAST NAME	RECEIVING BANK NAME
16107735722	DAVID	SMITH	Bank of America
diindiin@icloud.com	DAVID	SMITH	Bank of America
squiintzdealz@outlook.com	David	Smith	COASTAL COMMUNITY BANK
eaglesmith1066@gmail.com	HOPE	SMITH	Wells Fargo
squiintzzz@icloud.com	HOPE	SMITH	Wells Fargo
squiintzzz@icloud.com	HOPE	SMITH	Wells Fargo
squiintzdealz@outlook.com	David	Smith	COASTAL COMMUNITY BANK
16107735722	David	Smith	COASTAL COMMUNITY BANK
12153982824	David	Smith	Fulton Bank, N.A.
16107735722	DAVID	SMITH	Bank of America
squiintzzz@outlook.com	David	Smith	Fulton Bank, N.A.
16107735722	David	Smith	COASTAL COMMUNITY BANK

¹³ PayPal account ending 4560 connected using those IP Addresses during those dates.

76. On or around May 26, 2022, LegalZoom provided subpoena returns related to Squiintzzz Logistics LLC. A review of the returns identified customer David James Smith requesting LegalZoom to be the registered agent for Squiintzzz Logistics LLC in the commonwealth of Pennsylvania on or around April 1, 2022. SMITH's contact information was listed as: address 148 Arbor Way, Stroudsburg, Pennsylvania; email squiintzdealz@outlook.com; and phone number 610-773-5722. Additionally, the returns contained an IRS form SS-4, application for Employer Identification Number (EIN). Within the SS-4, SMITH and his Social Security Number were listed as the responsible party for Squiintzzz Logistics LLC. The mailing address on the SS-4 was 526 N. St. Cloud St. #665, Allentown, Pennsylvania. Further, the principal service of the business was described as "Consulting businesses on different ways to remain profitable & in Business." Squiintzzz Logistics was provided EIN ending 1105. SMITH was listed as the sole owner of Squiintzzz Logistics. Payments to LegalZoom were charged to Master Card with a number ending 3906.¹⁴¹⁵

77. On or around June 3, 2022, Law Enforcement received a package which bore tracking number ending 7091. The labels contained a sender address of Marlin Wayans 1711 Northampton St, Easton, PA. The package contained what appeared to a plastic bag containing a white powdery substance within a mylar bag that was within another mylar bag. On or around August 30, 2022, the DEA North Central Laboratory provided a report confirming the parcel contained around 1.52 grams of fentanyl and Xylazine¹⁶.

¹⁴ LegalZoom did not record the entire card number.

¹⁵ PayPal account ending 4560 had a Master Card ending 3906 with SMITH's name linked to the account

¹⁶ Xylazine is veterinary drug used as a sedative.

78. On or around June 16, 2022, an undercover employee placed an order within the dark net marketplace Tor2Door from vendor Squiintzzz for “7g top notch metch” for approximately 0.00593236 BTC (\$125) to be shipped via USPS.

79. On or around June 23, 2022, Pirate Ship provided new subpoena returns related to Squiintzzz. A review of the returns identified Account ID 2371325 was created on or May 22, 2022. Account information is in the table below. Payments for account 2371325 include credit card payment of Visa ending in 8630 and PayPal payment: diiindiin@icloud.com¹⁷.

Account	Email	Name	Address	Phone
2371325	diiindiin@outlook.com	James Todd	31 S 9 th St, 3, Allentown, PA ¹⁸	570-213-7854

Account 2371325 created around 248 labels to be shipped throughout the United States in May and June 2022. Those labels included the parcels Law Enforcement received with USPS tracking numbers ending 7091 and 4409 (discussed below).

80. On or around July 1, 2022, Law Enforcement received a package which bore tracking number ending 4409. The labels contained a sender address of James Todd, 19 hilktop dr, Wappingers Falls, NY. The package contained what appeared to a blue plastic bag containing a white crystalline substance within a blue plastic bag within a mylar bag that was within another mylar bag. On or around August 30, 2022, the DEA North Central Laboratory provided a report confirming the parcel contained around 8.383 grams of methamphetamine hydrochloride.

¹⁷ Same PayPal account previously mentioned.

¹⁸ Same address, except the 3, as address used for David Smith’s UPS profile, address associated to phone number 610-773-5722 under Ashley Lopez’s name, and diiindiin@icloud PayPal account.

81. On or around July 19, 2022, Law Enforcement received a police report regarding the arrest of SMITH by Stroud Area Regional Police Department, East Stroudsburg, Pennsylvania. Officers were dispatched to 148 Arbor Way, Stroudsburg, Pennsylvania, on July 4, 2022, for a domestic incident involving SMITH and “ex girlfriend” Ashley Lopez. When officers identified SMITH, they learned that SMITH had a warrant for a violation of parole and arrested him.

82. On or around July 20, 2022, Law Enforcement received inmate calls from Smithfield SCI, PA, where SMITH was being held. Two calls were received dated July 12, 2022, and July 15, 2022. Both calls are from SMITH to an unknown female using telephone number 908-836-4607. SMITH talks with the unknown female for approximately 14 minutes and approximately eight minutes respectively. SMITH tells the unknown female that he had been on the run for about two years and “Ashley called the cops on me”. SMITH tells the unknown female that Ashley has his iPhone and kept his money, his cars, and his dog. SMITH mentioned that he was the stepdad of a five-year-old named Alinda, who called SMITH “DinDin” (like “diindiin” as referenced from accounts above).

83. On July 22, 2022, Law Enforcement reviewed the profile of SquintzzzLogistics available within the darknet forum Dread. The profile advertised the “Squintzzz Logistics Private Vendor Store URL” and indicated that the vendor was also active at darknet marketplaces Tor2Door, Bohemia, ASAP, and Versus. The profile also showed that the vendor was inactive at the darknet marketplaces Incognito, Alphabay, Abacus, and Vice City (these marketplaces where Squintzzz stated he was inactive had been previously seized by law enforcement or stopped their services).

84. On the same date, Law Enforcement visited the profile of Squiintzzz within the Tor2Door marketplace, which showed that the user was last seen “2 weeks ago”. The profile also showed that the vendor had 312 total sales. Within the same profile, Squiintzzz advertised the following details regarding his sales record:

90 percent of vendors take at least a week. We get all orders to their destination within 5 days. Almost always less.

Sales:

Torrez (609)
93.1 % positive rating

Dark0de (513)
4.51/5 Star Rating

Tor2Door (300+)
4.9/5 Rating

Bohemia (100+)
97 % Positive Rating

We work hard to maintain these standards. We put the buyers first. Every time.

19

85. On the same day, Law Enforcement visited the profile of Squiintzzz within the ASAP darknet marketplace, which showed that the user was last active within the marketplace on July 3, 2022.

86. On July 25, 2022, Law Enforcement visited the profile of Squiintzzz within the Tor2Door darknet marketplace, which showed that the user was last seen “3 weeks ago”. Affiant believes Squiintzzz’s last seen dates on Tor2Door and ASAP marketplace are consistent with the date of SMITH’s arrest on July 4, 2022.

87. On or around August 16, 2022, Law Enforcement received a police report regarding a disturbance at 148 Arbor Way, Stroudsburg, Pennsylvania. Officers were dispatched to 148 Arbor Way on July 21, 2022, for an incident involving Grantland Aple and LOPEZ. LOPEZ was in her room at Arbor Way and told police that she does rent from Aple.

¹⁹ Torrez marketplace stopped operating on December 2021. Dark0de stopped operating on February 2022.

88. On August 25, 2022, Law Enforcement interviewed SMITH at the State Correction Institution (SCI) – Greene in Waynesburg, Pennsylvania. SMITH stated he did not know anything about the darknet. After being shown an image²⁰ believed to be SMITH carrying parcels bought from Squiintzzz and telling SMITH that Law Enforcement had legal documents connecting his name to Squiintzzz Logistics, LLC registered in the Commonwealth of Pennsylvania, SMITH asked if Law Enforcement thought he would be dumb enough to connect his personal information with a darknet moniker and that Law Enforcement would not find any of his fingerprints inside any of the parcels Law Enforcement received. SMITH then requested an attorney.

89. On or around September 6, 2022, Law Enforcement received jail calls from the SCI – Smithfield in Huntingdon, Pennsylvania for inmate SMITH. The calls were from around July 12 to August 13, 2022. A review of the calls identified SMITH calling Hope Smith, his mom, phone number 215-868-2377. On August 10, 2022, SMITH called 215-868-2377 and his mother answered. She stated she was with Ashley and SMITH asked her to put Ashley on the phone. Affiant believes Ashley is Ashley LOPEZ. SMITH then talked with LOPEZ. SMITH told LOPEZ it was hard to get a hold of her and he wrote her nine letters, but LOPEZ said she only got four or five of them. Later in the call, LOPEZ said when SMITH “went”, Affiant believes went refers to when SMITH was arrested in July 2022, there was only about \$2,000 in cash left, but SMITH said there was supposed to be \$3,500 in cash and \$1,600 in Cash App. LOPEZ stated that after SMITH went, she went into the room to grab what she could, but someone stole SMITH’s Cash App card. Additionally, Grant told LOPEZ that SMITH’s debt was LOPEZ’s

²⁰ The image was the image of the white male carrying boxes described previously in this affidavit.

debt, so she owed Grant money. LOPEZ stated she gave him almost \$1,000, but he was not happy and kicked LOPEZ out. Affiant believes that Grant is Grantland Aple, who SMITH was paying rent to at Arbor Way.

90. Later in the call, LOPEZ stated “they” stole the safe and they took all “your s**t.” SMITH asked if they took all of it including his computers. LOPEZ responded saying she has the computer. SMITH later stated, “don’t worry about what you got left because listen, I have crypto hidden alright I need to explain to you how to get it.” Later in the call, LOPEZ asked SMITH if he wrote the code to the safe. Affiant believes LOPEZ is referring to writing the code in the jail letters from SMITH to LOPEZ. SMITH said he did and LOPEZ responded, “I knew it. That’s why they took that fucking shit.” SMITH then responded, “Wait you don’t have none of the ice left?” LOPEZ responded “No everything was in there...I weighed it. It was 155. 155 plus whatever we had left which I think you said it was a quarter, it was a lot it was a lot, I know I didn’t even touch the ice. I called R.” SMITH told her, “That’s what I was going to say to you. Tell that mother fu***r what they did.” LOPEZ stated “I did but he, he he talked to Grant and Grant tried to smooth it over... 155 grams was the biggest we’ve ever had...” Affiant believes LOPEZ is telling SMITH that Grant read the code to their safe and stole everything inside including 155 grams of methamphetamine, also called ice, and a quarter kilogram of another kind of narcotic. Additionally, Affiant believes that “R” is one of their narcotic suppliers.

91. Later in the same call, SMITH told LOPEZ he is sending an important letter to Lehigh street. SMITH said “Listen, so I’m gonna tell you and I’m going to help you listen there’s still it’s not it’s not over yet. I’m going to have to have you bring operations back up...It’s not going to be easy...You have the most important thing which is my computer...”

LOPEZ responded, “that was the first thing I grabbed.” Affiant believes the “operations” SMITH was going to have LOPEZ bring back up was selling narcotics on the darknet.

92. On or around September 12 and 27, 2022, Law Enforcement received jail calls from SCI Greene for inmate SMITH. The calls were from around August 17 to September 20, 2022. A review of the calls identified around August 22, SMITH talked with LOPEZ and told LOPEZ he owed “R” 11,000 because he paid him four stacks before he got locked up. Affiant believes SMITH meant he owed “R” \$11,000. Later in the call, LOPEZ said, “you said you had the money for me in crypto or something. How do I get it?” SMITH replied that “it’s all in the market.” Additionally, he stated “this money on this markets, I don’t know what the climate is. Like, I don’t know if anybody exit scammed. You know what I mean? So, it’s got to happen sooner rather than later.” Based on my training and experience, Affiant knows that an exit scam on darknet marketplaces occurs when administrators of the marketplace close the market without warning and steal all the cryptocurrency that buyers and vendors had stored on the market. Affiant believes SMITH still had cryptocurrency on marketplaces when he was arrested in July and wanted LOPEZ to retrieve the cryptocurrency before an exit scam occurred on the market.

93. In another call on or around September 6, LOPEZ told SMITH that she did not realize that the kids’ iCloud accounts were linked to SMITH’s diiindiiin iCloud account and the kids kept changing the passcode. LOPEZ said she no longer knows what his diiindiiin iCloud account is anymore. SMITH tried to tell LOPEZ the password, but LOPEZ said that is not it anymore. Affiant believes the diiindiiin iCloud account is the diiindiiin@icloud.com email account mentioned previously in this affidavit.

94. On or around September 18, LOPEZ told SMITH in a jail call that she overdosed yesterday or the night before. She said the police used Narcan on her. SMITH told her he did not

have to use Narcan on her the two times he had to bring her back. He said the second time he was within seconds of calling to get her Narcan because she was not moving at all.

95. On or around September 27, 2022, Law Enforcement received letter communications from SCI Greene for inmate SMITH. The communications included multiple letters from LOPEZ to SMITH. Around August 2022, LOPEZ wrote, "...demanding Grant tell me who did this bc he didn't understand the severity of losing something that wasn't ours yet! A couple days ago I moved the pack into the safe (ice was there already) bc I wasn't sure where exactly to hide it...the safe was the safest place. I had about 8 gm on me to keep some sort of change coming in and wouldn't touch anymore in case it needed to be returned to R". In another letter dated August 15th, LOPEZ wrote, "I hope I speak to you soon. I need to know what and when and how I'm going to start things up again. I texted R saying simply lol spoke w/ you finally and you said about me getting things running again but no answer (it's been like that since I told him about Grant and Bianca stealing everything and anything I had left behind..." Affiant believes LOPEZ was writing about the narcotics that were stolen out of the safe at the Arbor Way residence. Additionally, Affiant believes LOPEZ meant she kept eight grams of drugs with her to try and sell for some money. Affiant further believes LOPEZ was trying to get additional narcotics from "R" to sell.

96. On or around September 27, 2022, Law Enforcement received email communications from JPay Inc. for SCI Greene inmate SMITH. A review of the emails identified communications between LOPEZ and SMITH from around August 2022 and September 2022. On or around August 20, LOPEZ emailed SMITH, "All my stuff that wasn't stolen is just sitting by a garage area hoping it's not taken away. Tell me Dave what the fuck am I to do now?? Setting up any operations is out of the question right now because I don't have

anywhere to even hook up the computer". Affiant believes LOPEZ was discussing not being able to set back up the Squiintzzz darknet drug operation. Additionally, on or around September 17, LOPEZ emailed SMITH "I od last night". Affiant believes this is the same overdose that LOPEZ talked with SMITH via jail calls about in which LOPEZ stated that police officers used Narcan on her.

97. On or around November 4, 2022, Apple Inc. provided search warrant returns for iCloud content for squiintzzz@icloud.com and diiindiiin@icloud.com. A review of the returns identified photographs within both accounts of SMITH and LOPEZ including a photograph of LOPEZ while she is holding her Pennsylvania drivers license. Additionally, there were photographs of various narcotics including what appeared to be methamphetamine, LSD, and fentanyl, and pills. One of the photographs, shown below, shows SMITH holding a bag of white crystals to his face. Affiant believes the crystals are consistent with methamphetamine.



Another photograph, shown below, shows a piece of cardboard with name Squiintzzz, 2-25, Kingdom, Vice City, and ASAP²¹ written on it. On top of the cardboard are blue stamped wax paper in small plastic baggies including wax paper with “drive thru” on it. The baggies and wax paper appear similar to the “10 bags of drive thru stamped china white pure!!! clone” an undercover employee purchased from Squiintzzz on or around January 31, 2022, that tested positive for fentanyl. Affiant knows that darknet vendors utilize photographs like this to prove they have the narcotics they are selling.



²¹ Kingdom, Vice City, and ASAP are darknet marketplaces known to law enforcement.

98. Further review of the iCloud returns identified four email messages within the diindiiin@icloud.com account that listed BTC address "...Ap4C1". Two were sent to diindiiin@icloud.com, one was sent to diindiiin@outlook.com, and one was located within the "Draft" folder of the account. The BTC address "...Ap4C1" was the same address the undercover employee used to purchase "1g of Synthetic China White" on or around May 8, 2022.

99. For the foregoing reasons, Affiant respectfully submits that there is probable cause that DAVID JAMES SMITH violated 21 U.S.C. § 841(a)(1) and (b)(1)(C), distribution of a controlled substance, on diverse occasions from at least November 2021 to June 2022, and 21 U.S.C. § 843(c)(2)(A), using the Internet to offer to distribute a controlled substance from at least September 2021 to July 2022.



Shadron Starnes
Special Agent
Federal Bureau of Investigation

This affidavit was sworn to by the affiant by telephone after a PDF was transmitted by email, per Fed. R. Crim. P. 3, 4(d), and 4.1, this 19th day of December 2022.



JONATHAN D. GREENBERG
U.S. MAGISTRATE JUDGE